*International Journal For Technological Research In Engineering*
*Volume 5, Issue 9, May-2018* *ISSN (Online): 2347 - 4718*

# TEES: AN EFFICIENT SEARCH SCHEME OVER ENCRYPTED DATA ON MOBILE CLOUD

N.J.Lokesh[1], Mr.P.G.Gopinath[2]
[1]PG Scholar, [2]Assistant Professor M.E., (Ph.D.)
GRT Institute of Engineering and Technology, Tiruttani, India.

***ABSTRACT: Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging. In this paper, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade whenthe performance enhancement methods are applied. Our experiments show that TEES reduces the computation time by 23% to 46% and save the energy consumption by 35% to 55% per file retrieval, meanwhile the network traffics during the file retrievals are also significantly reduced.***

## I. INTRODUCTION

Cloud storage system is a service model in which data are maintained, managed and backup remotely on the cloud side, and meanwhile data keeps available to the users over a network. Mobile Cloud Storage (MCS) denotes a family of increasingly popular on-line services, and even acts as the primary file storage for the mobile devices.

MCS enables the mobile device users to store and retrieve files or data on the cloud through wireless communication, which improves the data availability and facilitates the file sharing process without draining the local mobile device resources. The data privacy issue is paramount in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud, and data users retrieve the interested data by encrypted search scheme.

In MCS, the modern mobile devices are confronted with many of the same security threats as PCs, and various traditional data encryption methods are imported in MCS. However, mobile cloud storage system incurs new challenges over the traditional encrypted search schemes, in consideration of the limited computing and battery capacities of mobile device, as well as data sharing and accessing approaches through wireless communication.

Therefore, a suitable and efficient encrypted search scheme is necessary for MCS. Generally speaking, the mobile cloud storage is in great need of the bandwidth and energy efficiency for data encrypted search scheme, due to the limited battery life and payable traffic fee. Therefore, we focus on the design of a mobile cloud scheme that is efficient in terms of both energy consumption and the network traffic, while keep meeting the data security requirements through wireless communication channels.

MCS Challenges and Design
Efficiency Challenges:
Note that traditional file search and retrieval schemes, such as TRS, can provide data security but at the cost of more complicated procedures than Plain Text Search (PTS). TRS has been widely employed in cloud storage systems, but the encryption and the ranking incur the heavy calculation cost on a mobile device, and thus introduce the new challenges in efficiency for MCS traffic and energy consumption. It is communication. Therefore, a suitable and efficient encrypted search scheme is necessary for MCS.

Generally speaking, the mobile cloud storage is in great need of the bandwidth and energy efficiency for data encrypted search scheme, due to the limited battery life and payable traffic fee. Therefore, we focus on the design of a mobile cloud scheme that is efficient in terms of both energy consumption and the network traffic, while keep meeting the data security requirements through wireless communication channels. To this end, we introduce TEES (Traffic and Energy saving Encrypted Search) architecture for mobile cloud storage applications.

TEES achieves the efficiencies through employing and modifying the ranked keyword search as the encrypted search platform basis, which has been widely employed in cloud storage systems. Traditionally, two categories of encrypted search methods exit, that can enable the cloud server to perform the search over the encrypted data

## II. RELATED WORKS

1.TITLE: A break in the clouds: towards a cloud definition
AUTHORS: L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner Securely processing data in the cloud is still a difficult problem, even with homomorphic encryption and other privacy preserving schemes. Hardware solutions provide additional layers of security and greater performance over their software alternatives. However by definition the cloud should be flexible and adaptive, often viewed as

abstracting services from products. By creating services reliant on custom hardware, the core essence of the cloud is lost. FPGAs bridge this gap between software and hardware with programmable logic, allowing the cloud to remain abstract. FPGA as a Service (FaaS) has been proposed for a greener cloud, but not for secure data processing. This paper explores the possibility of Secure FaaS in the cloud for privacy preserving data processing, describes the technologies required, identifies use cases, and highlights potential challenges.

2.TITLE: Design of security solution to mobile cloud storage AUTHORS: X. Yu and Q. Wen With the increasing computation and storage capabilities of mobile devices, the concept of fog computing was proposed to tackle the high communication delay inherent in cloud computing, and also improve the security to some extent. This paper concerns with the privacy issue inherent in the sustainable fog computing platform. However, there is no universal solution to the privacy problem in fog computing due to the device heterogeneity. In this paper, we proposed a differential privacy-based query model for sustainable fog computing supported data center. We designed a method that can quantify the quality of privacy preserving through rigorous mathematical proof. The proposed method uses the query model to capture the structure information of the sustainable fog computing supported data center, and the datasets for the query result are mapped to real vectors. Then, we implemented the differential privacy preserving by injecting Laplacian noise. The experiment results demonstrated that the proposed method can effectively resist various popular privacy attacks, and achieve relatively high data utility under the premise of better privacy preserving.

3.TITLE: Mobile cloud computing AUTHORS: D. Huang

With traditional server, it's difficult to upgrade, maintain, manage and expansion our deployed applications, and also the development cost is high. These are the key issues that affect the mobile terminal performance of compute-intensive applications. To solve these problems, we design and implement an online translation system based on android platform, which is combined with mobile cloud computing related technologies. We elaborate develop models and methods for compute-intensive oriented applications, which provide effective solutions and reference for compute-intensive applications.

4.TITLE: Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storageAUTHORS: O. Mazhelis, G. Fazekas, and P. Tyrvainen

The volume of worldwide digital content has increased nine-fold within the last five years, and this immense growth is predicted to continue in foreseeable future reaching 8ZB already by 2015. Traditionally, in order to cope with the growing demand for storage capacity, organizations proactively built and managed their private storage facilities. Recently, with the proliferation of public cloud infrastructure offerings, many organizations, instead, welcomed the alternative of outsourcing their storage needs to the providers of public cloud storage services. The comparative cost-efficiency of these two alternatives depends on a number of factors, among which are e.g. the prices of the public and private storage, the charging and the storage acquisition intervals, and the predictability of the demand for storage. In this paper, we study how the cost-efficiency of the private vs. public storage depends on the acquisition interval at which the organization re-assesses its storage needs and acquires additional private storage. The analysis in the paper suggests that the shorter the acquisition interval, the more likely it is that the private storage solution is less expensive as compared with the public cloud infrastructure. This phenomenon is also illustrated in the paper numerically using the storage needs encountered by a university back-up and archiving service as an example. Since the acquisition interval is determined by the organization's ability to foresee the growth of storage demand, by the provisioning schedules of storage equipment providers, and by internal practices of the organization, among other factors, the organization owning a private storage solution may want to control some of these factors in order to attain a shorter acquisition interval and thus make the private storage (more) cost-efficient.

5.TITLE: Virtualized in-cloud security services for mobile devices AUTHORS: J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian,

In this paper we present a set of policy-driven security protocols for ensuring the confidentiality and integrity of enterprise data in mobile cloud computing environments. The proposed protocols leverage trusted authority entities and the “elastic” virtualized nature of the cloud computing model to provide energy-efficient key management mechanisms and policy-driven data protection techniques that support the secure interaction of the mobile client with an assortment of cloud software and storage services. The main contribution lies in: (1) Offloading the intensive asymmetric key agreement mechanisms from the mobile client and delegating them to resource-lucrative trusted authority sites. This is achieved by aggregating the security associations, required to agree on symmetric keys between the client and the cloud services, in a single security association between the client and the trusted authority. The aggregation concept results in major energy savings especially when the client consumes a relatively large set of services as is the case in cloud computing today. (2) Designing a customizable policy-based security architecture that considers the sensitivity of cloud data to provide multi-level and fine-grained data protection methodologies that suit the energy-limited mobile devices and the low-bandwidth wireless networks characterizing current mobile cloud computing models. The system is implemented in a real cloud computing environment and the savings in terms of energy consumption and execution time are analyzed.

## III. PROPOSED SYSTEM

In this project, Proposed a one-to-one mapping OPE which will lead to Statistics Information Leak Control Wang et al. Proposed a one-to-many mapping OPE They implemented a complicate algorithm for security protection. However, their performance and energy consumption would a problem since their algorithm was complicate and need much computing resource. Proposed a confidentiality preserving rank ordered search. This scheme displays low performances as the relevance scores are computed on the client side, increasing its workload. Proposed a one round trip search scheme which could search the encrypted data. It worth noticing that multi keyword ranked search may incur more serious.

ADVANTAGE:

The advantages of the TEES design in terms of relevance score calculation offloading, and thus leads to reduction of file search and retrieval process.

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system.

- The output form of an information system should accomplish one or more of the following objectives.
- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

## IV. IMPLEMENTATION

DATA OWNER

In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database. In this module, any of the above mentioned person have to login, they should login by giving their email id and password.

USER

In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database. If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

STOP WORDS:

The target document text is tokenized and individual words are stored in array. A single stop word is read from stop word list. The stop word is compared to target text in form of array using sequential search technique. If it matches, the word in array is removed, and the comparison is continued till length of array.

After removal of stop word completely, another stop word is read from stop word list and again algorithm runs continuously until all the

Stop words are compared.

STEMMING:

Stemming is the process of reducing inflected (or sometimes derived) words to their word stem, base or root form—generally a written word form. The stem need not be identical to the morphological root of the word; it is usually sufficient that related words map to the same stem, even if this stem is not in itself a valid root.

TF-IDF (Relevance Count)

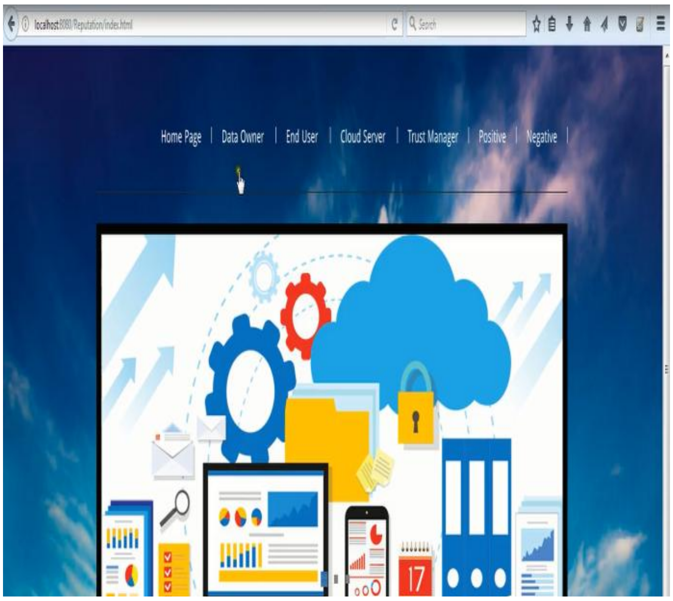
In information retrieval, tf–idf, short for term frequency–inverse document frequency, is a numerical statistic that is intended to reflect how important a word is to a document in a collection or corpus. Nowadays, tf-idf is one of the most popular term-weighting schemes. Variations of the tf–idf weighting scheme are often used by search engines as a central tool in scoring and ranking a document's relevance given a user query. tf–idf can be successfully used for stop-words filtering in various subject fields including text summarization and classification. One of the simplest ranking functions is computed by summing the tf–idf for each query term; many more sophisticated ranking functions are variants of this simple model.

CLOUD SERVER

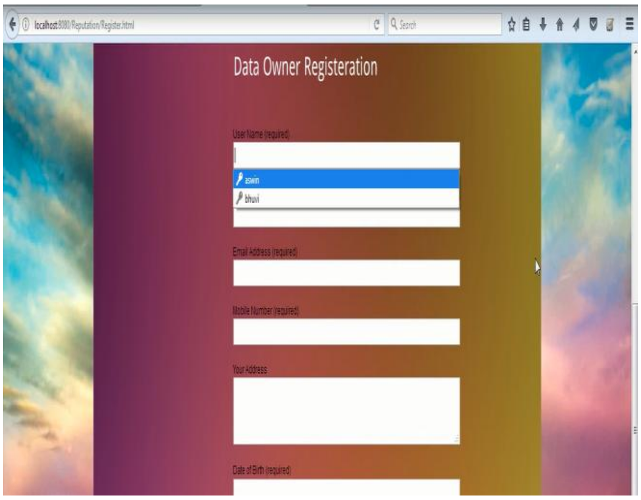
In this module cloud server view data owners and data user's details also. Server contains the all file details. In this server all files are stored in encrypted format using DES encryption.

## V. RESULTS

HOME PAGE


localhost:8080/Reputation/index.html
Search
Home Page | Data Owner | End User | Cloud Server | Trust Manager | Positive | Negative |

DATA OWNER REGISTRATION



Data Owner Registeration

User Name (required)

aswin
bhuvi

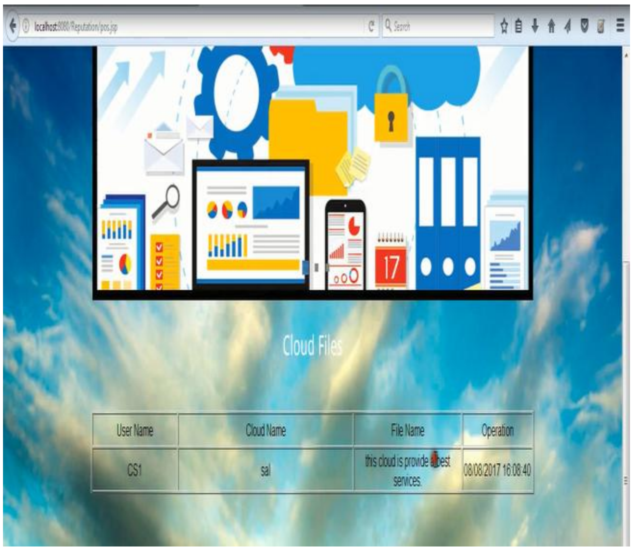
Email Address (required)

Mobile Number (required)

Your Address

Date of Birth (required)

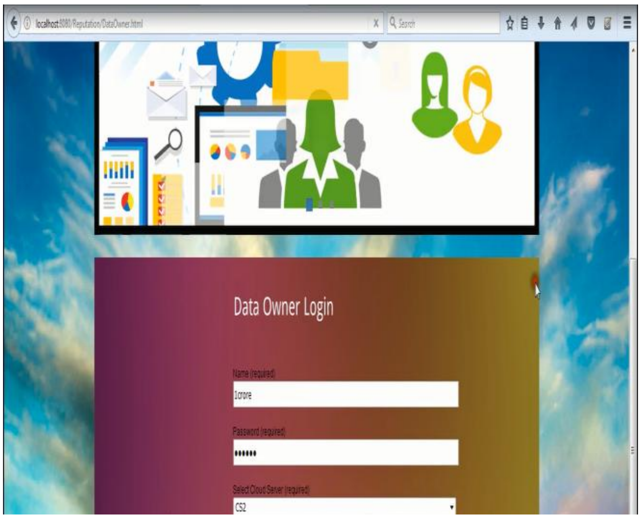
CLOUD SERVER FEEDBACK



Cloud Files

| User Name | Cloud Name | File Name | Operation |
|---|---|---|---|
| CS1 | sal | this cloud is provide a best services. | 08/08/2017 16:08:40 |

DATA OWNER LOGIN



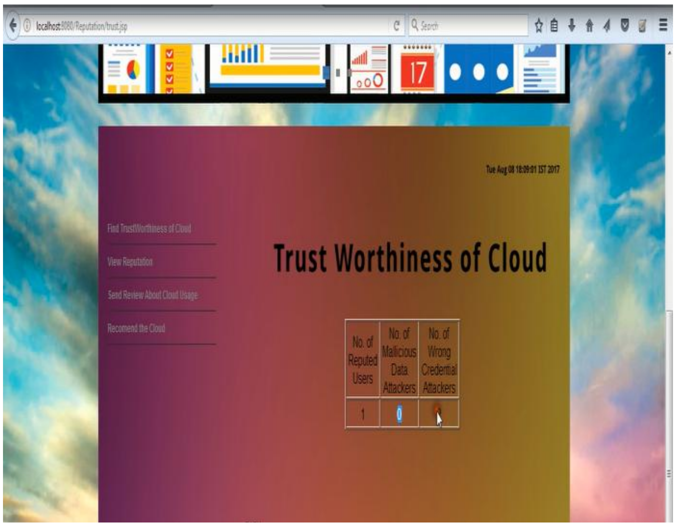
Data Owner Login

Name (required): 1crore

Password (required): ••••••

Select Cloud Server (required): CS2

TRUSTWORTHINESS OF CLOUD

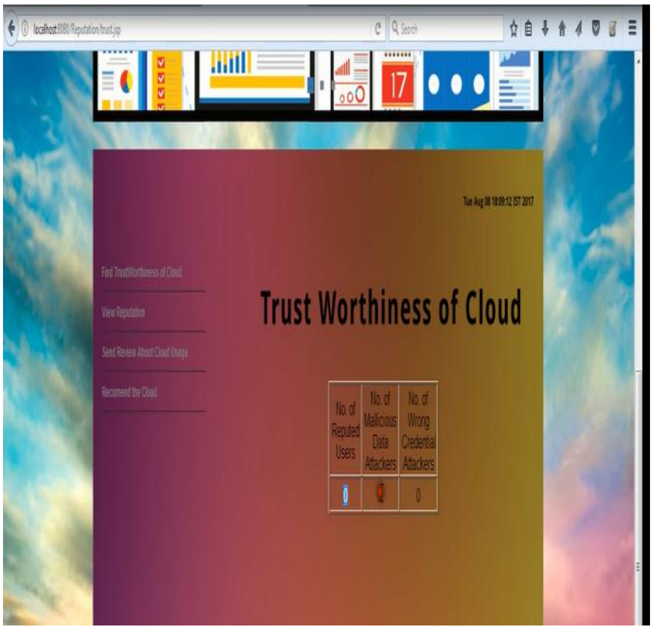

localhost:8080/Reputation/trust.jsp
Search
Find TrustWorthiness of Cloud
View Reputation
Send Review About Cloud Usage
Recomend the Cloud

Tue Aug 08 18:09:01 IST 2017

Trust Worthiness of Cloud

| No. of Reputed Users | No. of Malicious Data Attackers | No. of Wrong Credential Attackers |
|---|---|---|
| 1 | 0 | [illegible] |

RECOMMEND CLOUD SERVICE

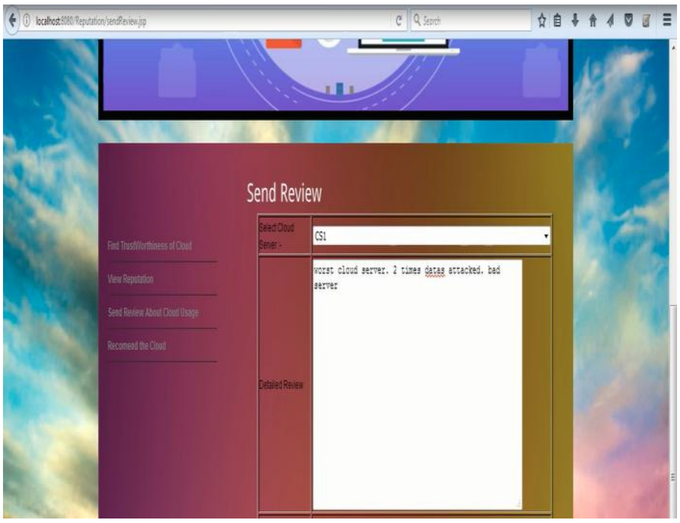

localhost:8080/Reputation/trust.jsp
Search
Find TrustWorthiness of Cloud
View Reputation
Send Review About Cloud Usage
Recomend the Cloud

Tue Aug 08 18:09:12 IST 2017

Trust Worthiness of Cloud

| No. of Reputed Users | No. of Malicious Data Attackers | No. of Wrong Credential Attackers |
|---|---|---|
| 0 | [illegible] | 0 |

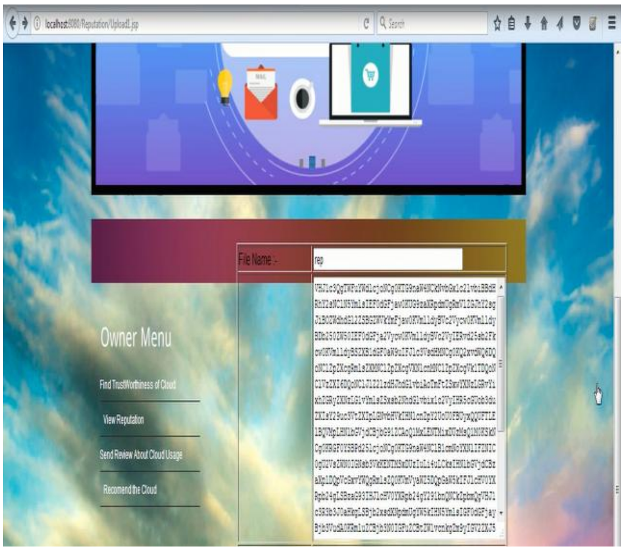
SEND REVIEW


localhost:8080/Reputation/sendReview.jsp
Send Review
Find TrustWorthiness of Cloud
View Reputation
Send Review About Cloud Usage
Recomend the Cloud

Select Cloud Server - CS1

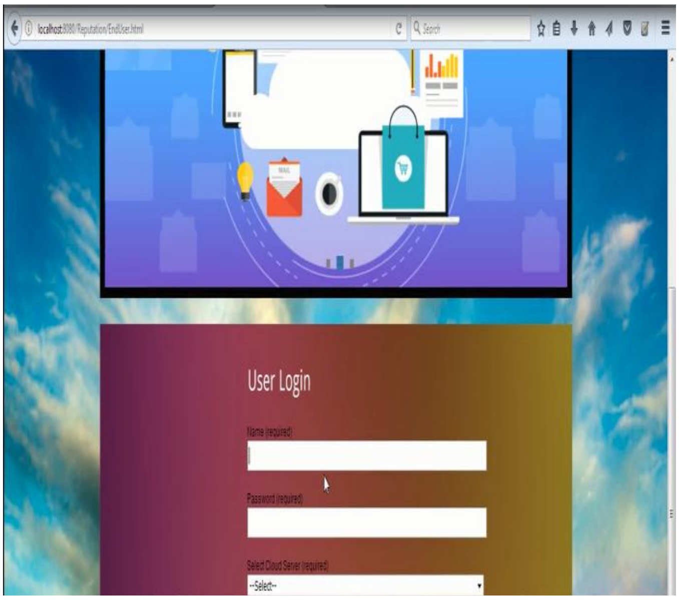
Detailed Review: worst cloud server. 2 times datas attacked. bad server

UPLOADED FILE IN ENCRYPTED FORMAT

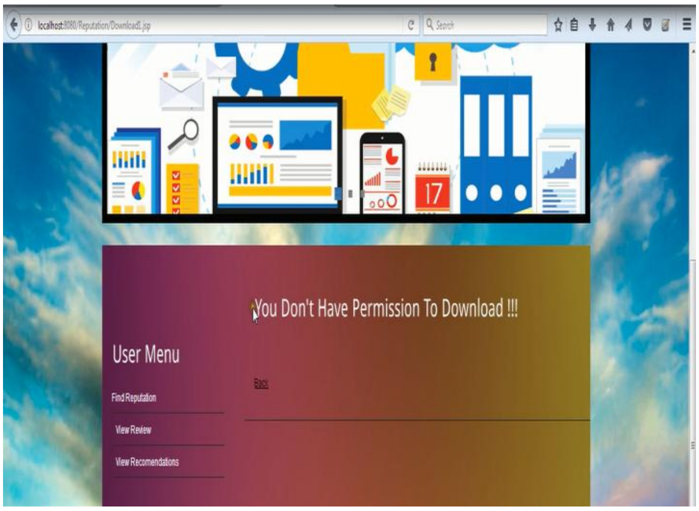

localhost:8080/Reputation/Upload1.jsp
Owner Menu
Find TrustWorthiness of Cloud
View Reputation
Send Review About Cloud Usage
Recomend the Cloud

File Name :- rep

USER LOGIN


localhost:8080/Reputation/EndUser.html
User Login
Name (required)
Password (required)
Select Cloud Server (required)
--Select--

DOWNLOAD FILE



You Don't Have Permission To Download !!!

## VI. CONCLUSION

In this project, we developed a new architecture, TEES as an initial attempt to create a traffic and energy efficient encrypted keyword search tool over mobile cloud storages. We started with the introduction of a basic scheme that we compared to previous encrypted search tools for cloud computing and showed their inefficiency in a mobile cloud context. Then we developed an efficient implementation to achieve an encrypted search in a mobile cloud. The security study of TEES showed that it is secure enough for mobile cloud computing, while a series of experiments highlighted its efficiency. TEES is slightly more time and energy consuming than keyword search over plain-text, but at the same time it saves significant energy compared to traditional strategies featuring a similar security level. Based on TEES, this work can be extended to more other novel implementations.

## REFERENCES

[1] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] X. Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[3] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[4] O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[5] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[6] J. Oberheide and F. Jahanian, “When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments,” in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.

[7] A. A. Moffat, T. C. Bell et al., Managing gigabytes: compressing and indexing documents and images. Morgan Kaufmann Pub, 1999.

[8] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Security and Privacy, 2000. S&P 2000. Proceedings.2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.